Computers, Materials & Continua
DOI: 10.32604/cmc.2023.032157
Article

Tech Science Press

Dipper Throated Optimization for Detecting Black-Hole Attacks in MANETs

Reem Alkanhel[1], El-Sayed M. El-kenawy[2,3], Abdelaziz A. Abdelhamid[4,5], Abdelhameed Ibrahim[6], Mostafa Abotaleb[7] and Doaa Sami Khafaga[8,*]

[1]Department of Information Technology, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh, 11671, Saudi Arabia
[2]Department of Communications and Electronics, Delta Higher Institute of Engineering and Technology, Mansoura, 35111, Egypt
[3]Faculty of Artificial Intelligence, Delta University for Science and Technology, Mansoura, 35712, Egypt
[4]Department of Computer Science, Faculty of Computer and Information Sciences, Ain Shams University, Cairo, 11566, Egypt
[5]Department of Computer Science, College of Computing and Information Technology, Shaqra University, 11961, Saudi Arabia
[6]Computer Engineering and Control Systems Department, Faculty of Engineering, Mansoura University, Mansoura, 35516, Egypt
[7]Department of System Programming, South Ural State University, Chelyabinsk, 454080, Russia
[8]Department of Computer Sciences, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, P.O. Box 84428, Riyadh, 11671, Saudi Arabia
*Corresponding Author: Doaa Sami Khafaga. Email: dskhafga@pnu.edu.sa
Received: 09 May 2022; Accepted: 09 June 2022

Abstract: In terms of security and privacy, mobile ad-hoc network (MANET) continues to be in demand for additional debate and development. As more MANET applications become data-oriented, implementing a secure and reliable data transfer protocol becomes a major concern in the architecture. However, MANET's lack of infrastructure, unpredictable topology, and restricted resources, as well as the lack of a previously permitted trust relationship among connected nodes, contribute to the attack detection burden. A novel detection approach is presented in this paper to classify passive and active black-hole attacks. The proposed approach is based on the dipper throated optimization (DTO) algorithm, which presents a plausible path out of multiple paths for statistics transmission to boost MANETs' quality of service. A group of selected packet features will then be weighed by the DTO-based multi-layer perceptron (DTO-MLP), and these features are collected from nodes using the Low Energy Adaptive Clustering Hierarchical (LEACH) clustering technique. MLP is a powerful classifier and the DTO weight optimization method has a significant impact on improving the classification process by strengthening the weights of key features while suppressing the weights of minor features. This hybrid method is primarily designed to combat active black-hole assaults. Using the LEACH clustering phase, however, can also detect passive black-hole attacks. The effect of mobility variation on detection error and routing overhead is explored and evaluated using the suggested approach. For diverse mobility situations, the results demonstrate

up to 97% detection accuracy and faster execution time. Furthermore, the suggested approach uses an adjustable threshold value to make a correct conclusion regarding whether a node is malicious or benign.

Keywords: Black-hole attack; mobile ad-hoc network; optimization; dipper throated optimization

1 Introduction

Recently, MANET becomes increasingly important for exchanging and extracting essential information for mobile network. It has a wide range of applications, from mobile sensing to military communications in battlegrounds, to name a few. A MANET is often characterized as a topology that changes over time. An ad-hoc network is made up of a group of distributed and decentralized infrastructures-less autonomous nodes with limited resources and broadcast channel sharing. Each node serves as both router and host, allowing non-neighboring nodes to be connected. These characteristics compel nodes to work together in data routing and forwarding. In contrast to wired networks, the behavior of nodes during data routing is unexpected and unknown, making MANET more vulnerable to various assaults. As a result, MANET security remains a work in progress, with several studies suggesting various countermeasures against a variety of attacks, including spying, distributed DoS (DDoS), denial of service (DoS), black-hole attack, and writing table overflow [1]. Sinking, spoofing, fabrication, and flushing are four different forms of assaults [2,3]. Sinking is the most malevolent node behavior, which occurs when one or more nodes in a network refuse to participate in routing operations and lose packets. A DoS attack is launched against sinking behavior [4]. Various detection and preventive approaches were developed and addressed in relation to this assault. A good sinking detection system, on the other hand, should be able to tell the difference between benign and malicious sinking because the dropping of benign packets in MANET can occur for a variety of reasons, including node mobility, heavy traffic, high network density and fading circumstances. Because of the node's heterogeneity and dynamic nature using traditional intrusion detection system (IDS) for MANET security poses several issues. Network congestion and routing delays also have an impact. The performance of IDS is challenged due to the randomization of transmission intervals and dynamic routing. As a result, in this situation, an intelligent routing algorithm is strongly advised. Sinker node activity may be identified by two characteristics: attack duration and packet dropping ratio (PDR). Since then, the intermittent sinking node behavior has been quite perplexing, especially when combined with benign packet dropping. After assessing these factors, a smart routing algorithm should be capable of determining the optimal path from the source to the destination and identify the sinker node.

In this paper, we present a novel optimization approach based on dipper throated optimization (DTO) to improve black-hole attack detection while reducing computation and time complexity. The originality of this work lies in the optimization of the parametric weight adjustment, which considerably reduces the computing cost and detection time when using machine learning algorithms. Furthermore, the proposed approach allows for a great deal of flexibility when it comes to altering the threshold value to discriminate between the benign sinker and malicious nodes.

2 Literature Review

Some of the most often used remedies to ad hoc networks and black-hole attack in MANETs are addressed in this section. Recent developments in this field have resulted in a slew of research [1]

that has yielded a slew of effective models and routing protocols. Securing the linkages in the network design, particularly over unsecured means, is one of the most crucial difficulties. Due to the restricted capacity of a node, earlier research has found that traditional security routines, including substantial calculations and communications overhead, are ineffective in MANETs [5–10]. As a result, a control mechanism should be put in place to ensure that authorized nodes only have network access. Secure Ad-hoc on-demand distance vector (SAODV) is among the most frequent detection techniques [10]. These techniques must include a security component based on a complicated encryption/decryption algorithm. Despite providing enough routing security to identify black-hole attacks, they consume much resources in the process of feigning a strong collaborative interaction among network nodes. Authors in [11] added a redundant routing protocol to validate whether a node is malicious or safe. The source node must unicast and get a ping to three different routes to the destination in order to use this strategy. The source node might validate each node and obtain a safe path to the destination after examining the responses to ping queries. This approach does not involve any additional malicious node processing, but it does necessitate a longer transmission latency.

A large portion of current MANET research is devoted to enhancing routing protocols based on various processes and establishing routing decisions on a range of constraints [12–16]. Furthermore, it has been demonstrated that making minor changes and adding new metrics to the operation and structure of routing protocols can enhance the security and performance of real-time applications [4]. One of these methods is the fuzzy inference system, which the authors built and compared the performance of AODV reactive routing protocol with and without it in [13], using a set of variables such as entropy function's information gain. Authors in [5] recently explored support vector machine (SVM) and classification trees techniques for identifying intrusions. The concepts of neuromorphic rules are used in developing another IDS model, which uses symbols rather than numeric values to determine each attack by indeterminacy, non-membership, and membership in a hybrid framework of genetic algorithms (GA) and self-organized features maps (SOFM) [14]. When employing this approach, the load of a network administrator, the required computations, and the communication overhead of the system remain major obstacles. Authors in [12] suggested a WOA-based intrusion detection system as well as a weak classification learner (decision stumps). In addition, [15] developed a method for identifying the black-hole attack by presuming the first route reply is from the rogue node and canceling the transaction. Despite the fact that this technology decreases data loss and improves speed, distinguishing between benign and malicious packet sinking is hard to achieve.

Despite the fact that many academics have concentrated on identifying passive black-holes, active black-hole assaults have received little attention. To identify black-hole attacks, authors in [16] introduced the first modified AODV routing protocol backed by SVM model. Their proposed methodology included a contingency table for each active transmission to keep track of the size of the packets transmitted. The transmitted packets from a source to destination nodes with and without black-hole from a basic network of seven nodes were monitored using a density curve with respect to time. Low peaks in the density curve were discovered to signal the discovery of one rogue node. However, additional data must be collected in order to identify the node with a black-hole and build comprehensive behavior proofs that include information from both data traffic and forwarding channels, as well as more evidence, in order to obtain a more accurate prediction result [17–19]. To improve the accuracy of SVM, the authors in [20] presented a particle swarm augmented SVM (PSO-SVM). As a result, authors in [21] proposed combining the Ant colony maximum and minimum optimization versions into SVM (i.e., ACO-SVM) based on the AODV routing protocol to identify only black-hole attacks of type passive in MANET. In an intrusion detection system, PSO-SVM was also used by the authors in [22] to identify packet dropping by passive black-holes. Machine

learning approaches are proposed by the authors in [23] for discriminating between normal and attacked network activity. In the feature selection process, these approaches were used: Packet Delivery Ratio, packet dropping, and end-to-end latency. As a result, machine learner settings have an impact on classification performance. Furthermore, because representative data differs not only from one problem to the next but also from one time to the next, the data collection procedure is critical. As a result, more representative data from biased data may be used to build a more effective machine learning model for a networking problem.

3 Proposed Approach

Active and passive black-hole attacks are the two most common forms of black-hole attacks. A large number of network nodes can be deceived when a routing message with extremely high power is broadcasted by a single malicious node. This process is known as a passive black-hole attack. It reroutes traffic and drops all packets as it passes through itself. As a result, this type of black-hole attack exclusively targets a network's architecture rather than introducing more fake routing signals into the network [24–30]. By receiving an instantaneous Route Reply Packet (RREP) packet, the malicious node persuades the entire adjacent node to submit their packets early in active black-hole attacks. The active black-hole node instantly sends a bogus RREP to the source node after receiving a Route Request Packet (RREQ), claiming to have a one-hop path to the destination [31]. Active and passive black-hole attacks are illustrated in Fig. 1. Data packets are usually delivered by source nodes after receiving the first RREP packet, and the remaining RREP packets will be dropped, as is typical of the AODV routing protocol. As a result, these unfiltered nodes attempt to utilize this malicious node as the next step in their routing route. They are, however, a long way from the target node, and obtaining a transaction requires numerous hops. Additional packets can be absorbed by the active black-hole node from other nodes and corrupting the routing information by implementing this scenario. As a result, the active black-hole node disrupts regular communication and significantly increases network demand. Consequently, it is far more challenging to detect or avoid than the passive black-hole [32], and it has far more undesirable effects on the network.

The proposed approach, on the other hand, is based on combining the benefits of both reactive and proactive routing strategies, as well as using an optimization algorithm to improve the accuracy of detecting the black-hole attacks of both types. The detection method is based on a careful examination of a set of key features that have been shown to be effective markers of active harmful conduct, as opposed to other factors that might be noisy data that detract from the detection decision's accuracy. Furthermore, using the dipper throated optimization (DTO) algorithm is used to optimize the parameter of a multi-layer perceptron network throughout the learning process for effective monitoring and detection of active black-holes attacks. A set of cluster head nodes is picked on a regular basis to collaborate in data aggregation and to develop exchangeable routing reply tables of trustworthy nodes in order to gather these properties. Based on the LEACH dynamic cluster head (CH) selection approach [33–35]. During the MANET lifetime, these clusters are regularly selected. Cluster-based routing has been shown to be an effective routing system for reducing communications, conserving node energy, and achieving load balance. Because of its changing structure, MANET presents additional routing issues. The LEACH approach, on the other hand, is a self-organized and self-adaptive cluster-based routing protocol that offers greater flexibility by inserting or removing nodes from clusters in each cycle. Every cluster consists of sensor nodes with the highest residual energy relative to other nodes, which are designated as CH, and the remaining nodes are designated as cluster members (CM). For the purpose of fulfilling the request, all nodes collaborate [36]. According to the previously established passive black-hole node behavior, the LEACH algorithm can identify

passive black-hole attacks since the CH that has unusually high power and does not transmit data all of the time is tagged as a black-hole one, and its chances of being picked are much lowered. Clustering occurs at regular intervals during the lifespan of the MANET, and it occurs in two stages: cluster setup and steady-state. The CH is selected during the setup phase, and data is detected during the steady-state phase. To decrease energy consumption, the steady-state stage has a substantially longer lifespan than the setup stage. Every round, CH is chosen using a mathematical formula that takes into account the total number of nodes in the cluster, the round number, and the CH probability (p) of each node. The workload of CH's is spread across all nodes over the lifespan of MANET by rotating their responsibilities, i.e., CH of the first round cannot be repeated in the future 1/p rounds [37]. This helps to balance the nodes' consumption of energy. After a specified period of time, the networks repeat the two processes to begin a new round. The CH is in charge of collecting information from the CMs once the clusters have formed. To avoid redundancy, the cluster head collects data and aggregates it. Each CH sends an advertising message to the other nodes, and each node chooses its CH depending on the signal strength of the message it received.

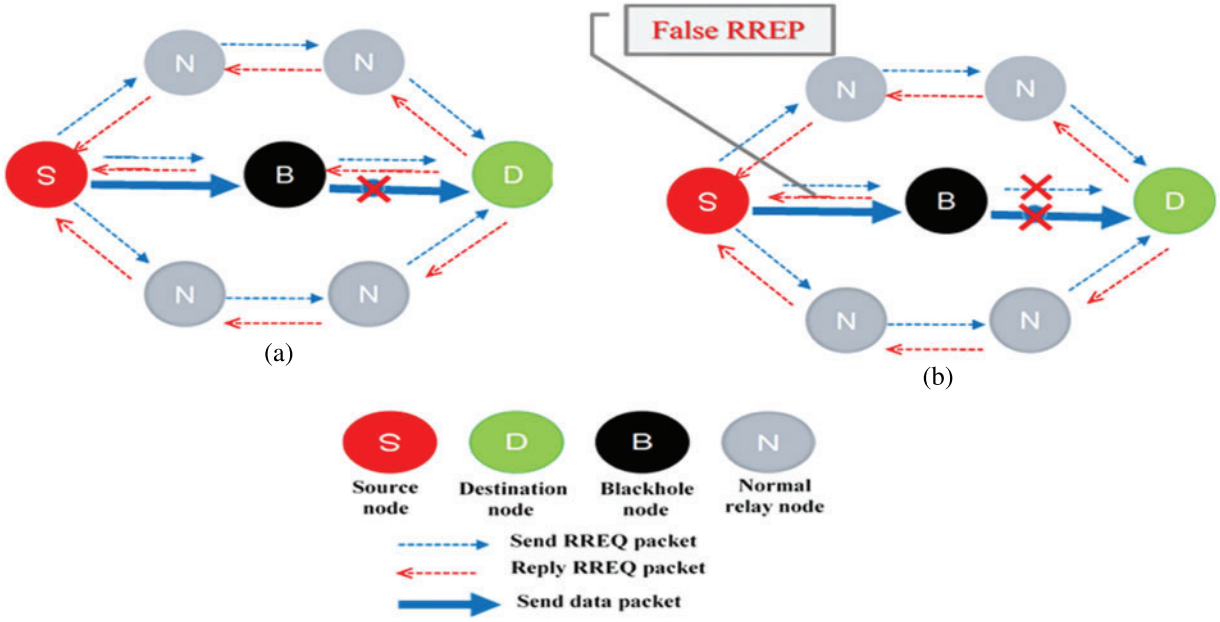


Figure 1: Black-hole attacks illustration; (a) Black-hole of type passive (b) Black-hole of type active

Finally, by sending a join message, CM are joined to the specified CH. The steady-state phase begins once the setup phase is completed and the data from each CH's CMs is gathered. By monitoring the delay variance of incoming packets entering each cluster during the data aggregation process at CHs, dropping behavior may be detected (called jitter value). This delay might be caused by benign factors like poor queuing, network congestion, configuration issues, or mobility, or by malicious node action. Each CH's job is to compare the gathered data to the underlying reason for the delay.

In each round, the proposed scheme works through two concatenating phases: (i) Data aggregation, which simulates the reactive protocol's process of collecting neighbors' node features, and (ii) Identification of malicious nodes, which analyzes the collected data using machine learning models. Furthermore, the multi-layer perceptron (MLP) machine learning classifier is adopted to classify the collected features. To achieve the best performance of MLP, the DTO optimization algorithm is

employed to optimize its connection weights. DTO plays a crucial role in enhancing the performance of MLP by suppressing or strengthening the weights of the neural network. MLP is a nonlinear machine learning technique that is particularly useful in the detection phase since it is a stable, robust classifier with high detection accuracy [38]. Throughout the lifespan of the MANET, the proposed approach will be performed at regular intervals.

3.1 Data Aggregation

Based on the estimated jitter value, this phase starts on occasion at CH of each suspicious cluster.

Step 1: Within the cluster, the CH node n_k transmits RREQ packets to its neighbors (where $k = 1, 2, \ldots, K$; where $K =$ suspicious clusters count). During the path discovery phase, the most likely path is selected from a list of many options. A multitude of pathways is possible for sending records from source to destination. It is critical to choose a unique path that transmits data effectively. Route request agent improves the routing table with statistics about pheromone value, hop count, and bandwidth when wandering to the destination. When the route request agent arrives at its destination, it is changed to route reply agent and forwarded in the form of acknowledgment closer to the original source. The route reply agent will follow the same path as the route request agent it is replying to.

Step 2: When RREQ packets are retrieved by a neighbor node, an RREP packet is generated as a response if it knows the destination. However, if the destination is unknown, the RREQ packets are multicasted to its neighbors to continue the route discovery process.

Step 3: Many information is contained in RREQ and RREP packets such as modified neighbors with a changed hop count, hop count, and other information. Sinker node always promotes the shortest path as the one with the smallest number of hops.

Step 4: A route reply table (RREPT) is built for each CH node n_k that contains critical features related to its neighbor node n_i ($i = 1, 2, \ldots, I$; where I is the count of CM in each cluster). The following are the properties:

i. The identification number of the destination node is D_{ID}.
ii. The RRE sent time is denoted by the initiation time (IT).
iii. The time at which the RREP was received is referred to as waiting time (WT).
iv. The end-to-end delay is measured by the difference between WT and IT.
iv. The identification number of the next-hop node is denoted by (NH).
v. To reach the destination, the hops count (HC) is used.
vi. Each neighbor node has a history of packet delivery rate referred to as (PDR).
vii. Within the cluster, each node has residual energy.

3.2 Identification of Malicious Nodes

The data analysis step begins when the RREPT has been finished. This phase examines the above-mentioned RREP properties in order to make a determination on whether nodes are malicious or benign.

Step 1: There are N observations taken during an interval ($i = 1, 2, \ldots, T$) under normal conditions and based on prior records, i.e., previous RREPT, for each feature F_j ($j = 1, 2, \ldots, J$; where

J is the total number of features). For each feature, the mean value c_{Fj} and the standard deviation δ_{Fj} values as measured as follow.

$$\mathrm{c_{F_j}} = \frac{1}{\mathrm{N}} \sum_{\mathrm{i=1}}^{\mathrm{N}} \mathrm{F_{ji}} \tag{1}$$

$$\delta_{F_j} = \sqrt{\frac{\sum_{i=1}^{N} (F_{ji} - c_{F_j})^2}{N}} \tag{2}$$

Step 2: Calculate the Euclidean distance d_j and the normalized feature value for each new item, as follows:

$$\overline{F_{ij}} = \frac{F_{ij} - \min F_j}{\max F_j - \min F_j} \tag{3}$$

$$d_j\left(\overline{F}_j, \mathrm{c_{F_j}}\right) = \sqrt{\sum_{i=1}^{N} \left(\overline{F}_{ji} - \mathrm{c_{F_j}}\right)^2} \tag{4}$$

The basis of parametric sampled data used in machine learners may be calculated using the formulae above.

Step 3: Using the sampled pairs ($\mathrm{F_{ij}}$, $\overline{F_{ij}}$) as input, apply DTO-MLP. Since the DTO module for weights adjustment is used, the agents are working in a semi-parametric manner. The feature weights are set to the same value as the original feature weights.

$$W_1(t) = \frac{1}{J} \tag{5}$$

The estimated MLP classifier error value ε is used to repeatedly update the new weights W_{t+1} of the sampled pairs ($\mathrm{F_{ij}}$, $\overline{F_{ij}}$) and the previous weights set W_t as follows:

$$W_{t+1} = \frac{W_t \exp\left(-\propto_t \overline{\mathrm{F_{ij}}} h_t\left(F_{ij}\right)\right)}{Z_t} \tag{6}$$

where:

$$\propto_t = \frac{1}{2} \log\left(\frac{1 - \varepsilon_t}{\varepsilon_t}\right) \tag{7}$$

and

$$h_t = \arg\ min_{h_j} \varepsilon_j = \sum\nolimits_{i=1}^{N} W_t(i) \tag{8}$$

The entire number of weights is represented by the number N. The stps of the proposed approach are shown in Algorithm 1.

Algorithm 1: The steps of the proposed DTO-MLP based approach

1: **Initialize** MANET
2: **While** MANET lifetime
3: **Initialize** DTO-MLP

(Continued)

Algorithm 1: Continued

```
Procedure DTO-MLP
  Select an initial point
    Iteration (t=1)
      Pheromones stretch
  Do until reaching stopping criterion
   For each bird
     Load locations and velocities
     Apply the Local Search
     Save the solution if it is the best one
    Update MLP weights:
   Loop
   Return the best weights
 % Apply LEACH algorithm
 For c =1, K:
  Compute jitter(c)
  If Jitter(c) <= stability threshold Do
  %Phase1: Data Aggregation
  Repeat n_i ≤I do
    Send RREQ
   Receive RREP
   Construct RREPT
  Until all nodes reply
  %Phase 2: Identification of Malicious Nodes
  For n_i ≤I do
   For j ≤ J do
     Compute ≤j, ≤j, F_ij (overline)
     Apply DTO+MLP
     Apply Phase 2 Step 3
     If detection = true
       Mark (n_i) as suspicious node
     End if
     End for
   End for
```

3.3 Dipper Throated Optimization Algorithm

The Dipper-Throated Optimization (DTO) approach is based on the idea of a flock of birds swimming about hunting for food. The position (P) and velocities (V) of the birds may be represented using the matrices below. The binary DTO is utilized to choose features, as previously stated.

The continuous DTO, on the other hand, is utilized to improve the classification neural network's parameters [39].

$$P = \begin{bmatrix} P_{1,1} & P_{1,2} & P_{1,3} & \ldots & P_{1,d} \\ P_{2,1} & P_{2,2} & P_{2,3} & \ldots & P_{2,d} \\ P_{3,1} & P_{3,2} & P_{3,3} & \ldots & P_{3,d} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ P_{m,1} & P_{m,2} & P_{m,3} & \ldots & P_{m,d} \end{bmatrix} \tag{9}$$

$$V = \begin{bmatrix} V_{1,1} & V_{1,2} & V_{1,3} & \ldots & V_{1,d} \\ V_{2,1} & V_{2,2} & V_{2,3} & \ldots & V_{2,d} \\ V_{3,1} & V_{3,2} & V_{3,3} & \ldots & V_{3,d} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ V_{m,1} & V_{m,2} & V_{m,3} & \ldots & V_{m,d} \end{bmatrix} \tag{10}$$

where the i^{th} bird in the j^{th} dimension is denoted by $P_{i,j}$ for $i \in 1, 2, 3, \ldots, m$ and $j \in 1, 2, 3, \ldots, d$. The bird's velocity in the j^{th} dimension for $i \in 1, 2, 3, \ldots, m$ and $j \in 1, 2, 3, \ldots, d$ is referred to as $V_{i,j}$. There is a uniform distribution of the beginning positions of $P_{i,j}$. For each bird, the values of the fitness functions $f = f_1, f_2, f_3, \ldots, f_n$ are determined using the array below.

$$f = \begin{bmatrix} f_1\left(P_{1,1}, P_{1,2}, P_{1,3}, \ldots, P_{1,d}\right) \\ f_2\left(P_{2,1}, P_{2,2}, P_{2,3}, \ldots, P_{2,d}\right) \\ f_3\left(P_{3,1}, P_{3,2}, P_{3,3}, \ldots, P_{3,d}\right) \\ \ldots \\ f_m\left(P_{m,1}, P_{m,2}, P_{m,3}, \ldots, P_{m,d}\right) \end{bmatrix} \tag{11}$$

The mother bird is the higher value, while each bird's hunt for food is represented in its fitness score. The values are sorted ascending, with P_{best} being declared the best answer. Normal birds are intended to be employed as follower birds, while P_{Gbest} has been dubbed the best solution. The optimizer's initial DTO strategy for updating the swimming bird's location is based on the equations that update the population's position and velocity:

$$P(i+1) = \begin{cases} P_{best}(i) - K_1.|K_2.P_{best}(i) - P(i)| & \text{if } R < 0.5 \\ P(i) + V(i+1) & otherwise \end{cases} \tag{12}$$

$$V(i+1) = K_3 V(i) + K_4 r_1 (P_{best}(i) - P(i)) + K_5 r_2 (P_{Gbest} - P(i)) \tag{13}$$

where $P(i)$ is the average bird position, $P_{best}(i)$ is the best bird position, and $V(i+1)$ is the bird's velocity at iteration $i+1$. The steps of DTO algorithm are represented by the flowchart shown in Fig. 2.

4 Experimental Results

NS-2 simulator ver. 2.35 is used to construct a MANET simulation environment on an Intel Core I5 CPU operating at 2.2 GHz with 8 GB of RAM and Ubuntu 20.04 operating system to test the proposed appraoch. The simulation was run on a 1500 m × 1500 m rectangular area with randomly dispersed mobile nodes and a constant bit rate (CBR) traffic source of a communication model. Tab. 1 lists all of the MANET settings. The suggested technique is put to the test in terms of detecting black-hole attacker nodes and overall detection time using various simulated scenarios. The robustness of the proposed detection technique is tested in these situations, which comprise several mobility modes.

The simulations in this research are run on various mobility speed situations to analyze and investigate the network's performance with and without the attack. The node speeds are set at 5 and 20 m/s, respectively. These nodes also travel in all directions at random. The evaluation metrics used in assessing the proposed approach are presented in Tab. 2.

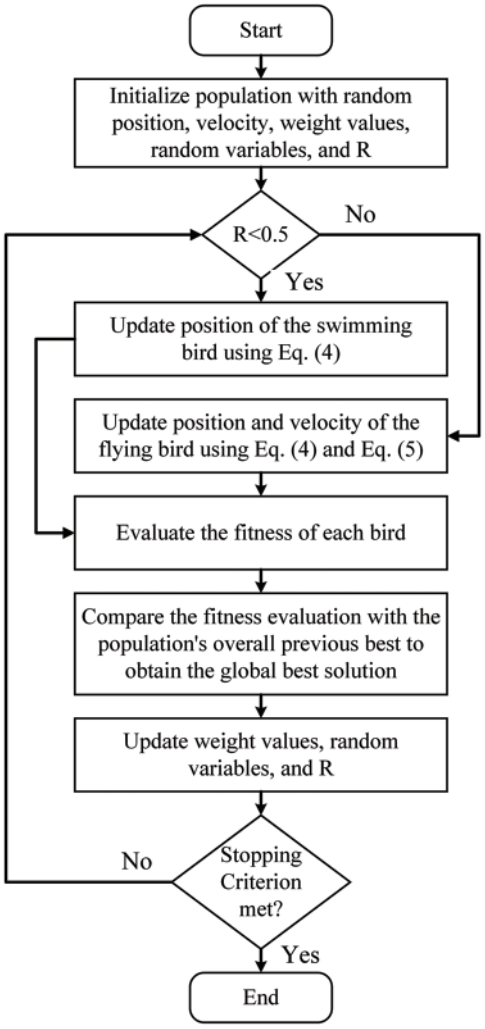


Figure 2: The algorithmic steps of the dipper throated optimization

Table 1: Simulation parameters of MANET

Parameter	Value
Routing protocol	AODV/LEACH
Simulation time	10 s
Pause time	1.0 s
Packet size	1000 Bytes/packet

(Continued)

Table 1: Continued

Parameter	Value
Scale of network	1500 m × 1500 m
MAC protocol	IEEE 802.11
MAC Type	802.11
Data Rate	0.1 Mbps
Node velocity	5, 20 m/sec
Node movement	Random
Node placement	Random
Antenna Model	Omni-Directional
Application traffic	CBR
No. of attackers	1/cluster
No. of source	1/cluster
Observation parameters	Throughput, end-to-end delay, Jitter
No. of mobile nodes	33 [3 clusters]

Table 2: Evaluation metrics

Metrics	Equation
Accuracy	$= \frac{(TN + TP)}{(TN + TP + FN + FP)}$
Recal	$= \frac{TP}{(TP + FN)}$
Precision	$= \frac{TP}{(TP + FP)}$
Specificity	$= \frac{TN}{(TP + FP)}$
F1-score	$= 2 * \frac{(Recall * Precision)}{(Recall + Precision)}$

On the other hand, to select the machine learning algorithm that can properly identify the network attacks, an experiment is conducted to compare the performance of three classifiers namely, Naïve bayes, decision tree, and MLP. The comparison results are presented in Tab. 3. These results show high performance achieved by MLP classifier. Therefore, we adopted this classifier for the conducted experiments.

Table 3: Comparing the performance of three machine learning models

	Naïve Bayes	Decision-tree	MLP
Accuracy	0.886075949	0.929133858	**0.948275862**
Sensitivity (TRP)	0.925925926	0.925925926	**0.957446809**
Specificity (TNP)	0.8	0.931506849	**0.909090909**
Pvalue (PPV)	0.909090909	0.909090909	**0.97826087**
Nvalue (NPV)	0.833333333	0.944444444	**0.833333333**
Fscor	0.917431193	0.917431193	**0.967741935**
Time (S)	15.6	13.2	**9.8**

In addition, the performance of MLP is boosted by optimizing the parameter of it using DTO algorithm. To show the superiority of this optimization, we analyzed and compared the results achieved by the optimized MLP using DTO and the optimization using four other optimizers namely, grey wolf optimizer (GWO), particle swarm optimizer (PSO), genetic algorithm (GA), and whale optimization algorithm (WOA). The results of this comparison are presented in Tab. 4. As shown in the table, the highest performance is achieved by the proposed DTO + MLP approach. The classification accuracy achieved is (97.5%) using the proposed approach, which is higher than the accuracy achieved by all other approaches.

Table 4: Comparison between the performance of five optimization algorithms

	DTO + MLP	GWO + MLP	PSO + MLP	GA + MLP	WOA + MLP
Accurcy	**0.975**	0.96875	0.966666667	0.965517	0.956522
Sensitivity (TRP)	**0.977653631**	0.971223022	0.968992248	0.967742	0.957447
Specificity (TNP)	**0.952380952**	0.952380952	0.952380952	0.952381	0.952381
Pvalue (PPV)	**0.994318182**	0.992647059	0.992063492	0.991736	0.989011
Nvalue (NPV)	**0.833333333**	0.833333333	0.833333333	0.833333	0.833333
F1-Score	**0.985915493**	0.981818182	0.980392157	0.979592	0.972973
Time	**2.8**	4.5	5.7	6.3	7.5

To highlight the effectiveness of the proposed approach, a statistical analysis is performed on the results achieved by the proposed approach and the other four approaches, and the results are recorded in Tab. 5. As presented in the table, all the criteria of the statistical analysis using the proposed approach outperform those of the other approaches.

On the other hand, the statistical difference between the proposed DTO + MLP and the other competing algorithms is explored. This analysis is carried out using a one-way analysis of variance (ANOVA) test. The major hypotheses in this test are the null and alternative hypotheses. For the null hypothesis H0 (i.e., DTO + MLP = GWO + MLP = PSO + MLP = GA + MLP = WOA + MLP), the algorithm's mean values are made equal. Under the alternative hypothesis, H1, the algorithms' means are not similar. The results of the ANOVA test are presented in Tab. 6.

Table 5: Statistical analysis of the performance of five optimization algorithms

	DTO + MLP	GWO + MLP	PSO + MLP	GA + MLP	WOA + MLP
Number of values	**14**	14	14	14	14
Minimum	**0.975**	0.9488	0.9467	0.9455	0.9365
Median	**0.975**	0.9688	0.9667	0.9655	0.9565
Maximum	**0.985**	0.9688	0.9667	0.9655	0.9565
Mean	**0.976**	0.9666	0.9645	0.9634	0.9544
Std. Error of Mean	**0.000749**	0.001547	0.001547	0.001547	0.001547
Std. Deviation	**0.002801**	0.005789	0.005789	0.005789	0.005789
25% Percentile	**0.975**	0.9688	0.9667	0.9655	0.9565
75% Percentile	**0.975**	0.9688	0.9667	0.9655	0.9565

Table 6: One way analysis of variance (ANOVA) test

	SS	DF	MS	F (DFn, DFd)	*P* value
Treatment	0.00335	4	0.000837	F (4, 65) = 29.50	$P < 0.0001$
Residual	0.001845	65	2.84E-05		
Total	0.005194	69			

The statistical difference between every two algorithms is used to determine the *p*-values between the proposed DTO + MLP method and the other competing algorithms, demonstrating that the recommended technique is considerably different. This study used Wilcoxon's rank-sum test. The two basic hypotheses in this test are the null and alternative hypotheses. For the null hypothesis represented by H0, DTO + MLP = GWO + MLP, DTO + MLP = PSO + MLP, DTO + MLP = GA + MLP, and DTO + MLP = WOA + MLP. Under the alternative hypothesis, H1, the algorithms' means aren't similar. The Wilcoxon rank-sum test's findings are shown in Tab. 7. As indicated in the table, the *p*-values of the proposed algorithm and the other algorithms are less than 0.05, demonstrating the superiority and statistical significance of the proposed DTO + MLP approach.

Table 7: Wilcoxon signed rank test

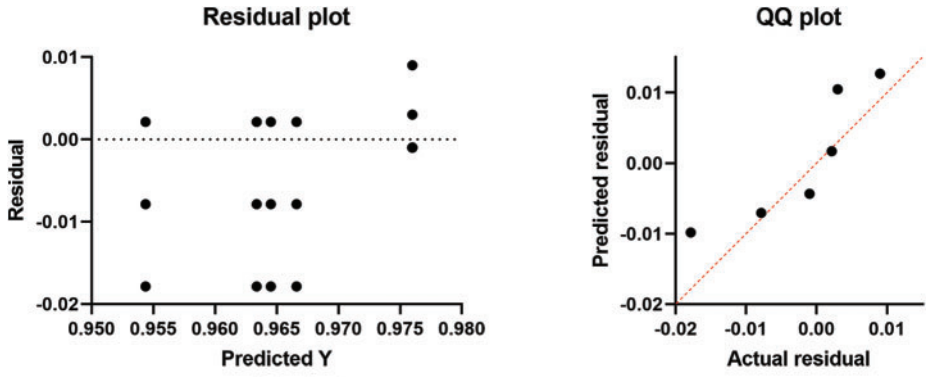
	DTO + MLP	GWO + MLP	PSO + MLP	GA + MLP	WOA + MLP
Theoretical median	**0**	0	0	0	0
Number of values	**14**	14	14	14	14
Actual median	**0.975**	0.9688	0.9667	0.9655	0.9565
Significant (alpha = 0.05)?	**Yes**	Yes	Yes	Yes	Yes

(Continued)

Table 7: Continued

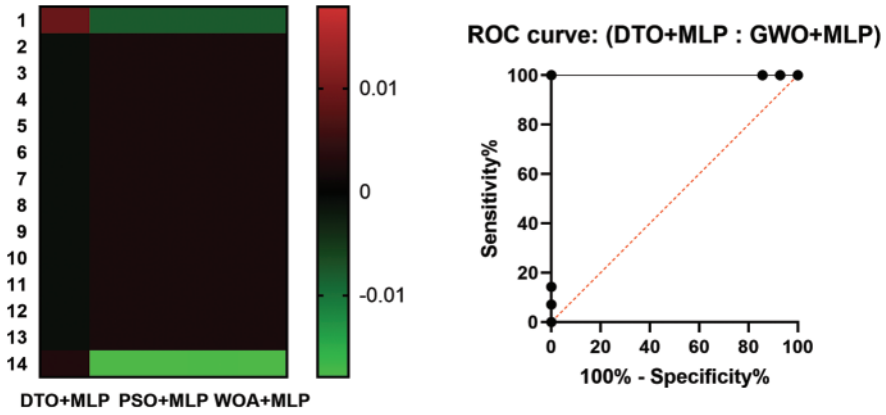
	DTO + MLP	GWO + MLP	PSO + MLP	GA + MLP	WOA + MLP
Sum of signed ranks (W)	**105**	105	105	105	105
Estimate or exact?	**Exact**	Exact	Exact	Exact	Exact
P value (two tailed)	**0.0001**	0.0001	0.0001	0.0001	0.0001
Sum of negative ranks	**0**	0	0	0	0
P value summary	***	***	***	***	***
Sum of positive ranks	**105**	105	105	105	105
How big is the discrepancy?					
Discrepancy	**0.975**	0.9688	0.9667	0.9655	0.9565

Fig. 3 shows a visual depiction of the findings obtained using the proposed method. The residual and QQ plots are the first two plots. The residual error in these graphs is in the region between −0.02 and 0.01, indicating that the proposed strategy is successful. Furthermore, the QQ plot demonstrates that the anticipated results match the actual values, emphasizing the superiority of the presented method. In addition, the last two plots, the heatmap and the area under curve (ROC) plot. These plots show the superiority and effectiveness of the proposed approach when compared with other approaches.



(a) Residual plot (b) QQ plot

Figure 3: (Continued)



(c) Heatmap plot (d) ROC curve

Figure 3: Visual representation of the achieved results

5 Conclusions and Future Directions

MANET routing based on clusters has been shown to be more efficient in terms of lifespan extension, load balancing, and attack resistance of the network. Despite the fact that dealing with MANET adds to the overhead of detecting attacks, the proposed approach has shown to be effective in terms of detection accuracy and time. The MLP classifier's complexity is further reduced by selecting the best set of transitions weights using the DTO algorithm, resulting in an accurate and quick detection system. However, because the suggested approach is based primarily on the accuracy of the data gathered from RREP packets, attacks based on packet modification are not examined in this paper. Furthermore, the LEACH algorithm can detect a passive black-hole attacks since a CH that does not transmit data all of the time is tagged as a black-hole one, with a low likelihood of being picked. However, detecting collaborative sinkholes that work together to create bogus requests might be difficult (i.e., RREQ and RREP). Multiple cooperating sinkhole nodes will be investigated in the future to expand this work, and additional attacks will be examined and tried utilizing the suggested approach.

Acknowledgement: Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2022R323), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Funding Statement: Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2022R323), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] S. Jangir and N. Hemrajani, "A comprehensive review and performance evaluation of detection techniques of black-hole attack in MANET," *Journal of Computer Science*, vol. 13, no. 10, pp. 537–547, 2017.

[2] V. Nassa, "Security vulnerabilities in mobile ad hoc networks," *International Journal of Science Technology and Managment*, vol. 2, no. May 2011, pp. 67–73, 2014.

[3] P. Yau and C. J. Mitchell, "Security vulnerabilities in ad hoc networks," in *Proc. of the 7th Int. Symp. Communication Theory and applications (ISCTA03)*, Ambleside, UK, pp. 2–7, 2003.
[4] S. Sarika, A. Pravin, A. Vijayakumar and K. Selvamani, "Security issues in mobile ad hoc networks," *Procedia of Computer Science*, vol. 92, pp. 329–335, 2016.
[5] M. Ektefa, S. Memar and L. S. Affendey, "Intrusion detection using data mining techniques," in *Int. Conf. on Information Retrieval & Knowledge Management (CAMP)*, Shah Alam, Selangor, pp. 200–203, 2010.
[6] M. Shaik and F. Mira, "A comprehensive mechanism of MANET network layer based security attack prevention," *International Journal of Wireless and Microwave Technologies*, vol. 10, no. 1, pp. 38–47, 2020.
[7] S. Marti, T. Giuli, K. Lai and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proc. of The 6th Annual Int. Conf. on Mobile Computing and Networking*, Boston Massachusetts, USA, pp. 255–265, 2000.
[8] A. El-Semary and H. Diab, "BP-AODV: Blackhole protected AODV routing protocol for MANETs based on chaotic map," *IEEE Access*, vol. 7, pp. 95197–95211, 2019.
[9] N. Dhanju, P. Khehra, E. Kumar and R. Garg, "Effect on various parameters under black-hole attack in MANETs using INRD Technique," *International Journal of Computer Science and Mobile Computing*, vol. 5, no. 6, pp. 343–349, 2016.
[10] Y. Ye, S. Feng, M. Liu, X. Sun, T. Xu *et al.,* "A safe proactive routing protocol SDSDV for ad hoc network," *International Journal of Wireless and Information Network*, vol. 25, no. 3, pp. 348–357, 2018.
[11] M. Adil, R. Khan, M. Almaiah, M. Al-Zahrani, M. Zakarya *et al.,* "MAC-AODV based mutual authentication scheme for constraint oriented networks," *IEEE Access*, vol. 8, pp. 44459–44469, 2020.
[12] M. Doja, B. Alam and V. Sharma, "Analysis of reactiverouting protocol using fuzzy inference system," in *AASRI Conf. on Parallel and Distributed Computing Systems*, Singapore, vol. 5, pp. 164–169, 2013.
[13] H. Elwahsh, M. Gamal, A. A. Salama and I. M. El-Henawy, "A novel approach for classifying MANETs attacks with a neutrosophic intelligent system based on genetic algorithm," *Security Communication Networks*, vol. 2018, pp. 1–10, 2018.
[14] A. Koujalagi, "Considerable detection of black-hole attack and analyzing its performance on AODV routing protocol in MANET (Mobile Ad Hoc Network)," *American Journal of Computer Science and Information Technology*, vol. 6, no. 2, pp. 1–6, 2018.
[15] A. Abdelhamid and S. Alotaibi, "Optimized two-level ensemble model for predicting the parameters of metamaterial antenna," *Computers, Materials & Continua*, vol. 73, no. 1, pp. 917–933, 2022.
[16] A. Abdelhamid, E. M. El-Kenawy, B. Alotaibi, G. Amer, M. Abdelkader *et al.,* "Robust speech emotion recognition using CNN+LSTM based on stochastic fractal search optimization algorithm," *IEEE Access*, vol. 10, pp. 49265–49284, 2022.
[17] B. Singh and S. Bansal, "A review: Intrusion detection system in wireless sensor networks," *International Journal of Computational Mathematics and Science*, vol. 6, no. 6, pp. 13–19, 2017.
[18] V. Kumar and R. Kumar, "An adaptive approach for detection of blackhole attack in mobile ad hoc network," *Procedia Computer Science*, vol. 48, no. 1, pp. 472–479, 2015.
[19] F. Ardjani, K. Sadouni and M. Benyettou, "Optimization of SVM multiclass by particle swarm (PSO-SVM)," in *2nd Int. Workshop on Database Technologies and Applications*, Wuhan, China, pp. 1–4, 2010.
[20] A. Ibrahim, H. A. Ali, M. M. Eid and E. -S. M. El-Kenawy, "Chaotic harris hawks optimization for unconstrained function optimization," in *2020 16th Int. Computer Engineering Conf. (ICENCO)*, Cairo, Egypt, IEEE, pp. 153–158, 2020.
[21] S. S. M. Ghoneim, T. A. Farrag, A. A. Rashed, E. -S. M. El-Kenawy and A. Ibrahim, "Adaptive dynamic meta-heuristics for feature selection and classification in diagnostic accuracy of transformer faults," *IEEE Access*, vol. 9, pp. 78324–78340, 2021.
[22] M. M. Eid, E. -S. M. El-Kenawy and A. Ibrahim, "A binary sine cosine-modified whale optimization algorithm for feature selection," in *4th National Computing Colleges Conf. (NCCC 2021)*, Taif, Saudi Arabia, pp. 1–6, 2021.

[23] A. A. Salamai, E. -S. M. El-kenawy and A. Ibrahim, "Dynamic voting classifier for risk identification in supply chain 4. 0," *Computers, Materials & Continua*, vol. 69, no. 3, pp. 3749–3766, 2021.
[24] E. -S. M. El-Kenawy, S. Mirjalili, S. S. M. Ghoneim, M. M. Eid, M. El-Said *et al.,* "Advanced ensemble model for solar radiation forecasting using sine cosine algorithm and Newton's laws," *IEEE Access*, vol. 9, pp. 115750–115765, 2021.
[25] E. -S. M. El-kenawy, H. F. Abutarboush, A. W. Mohamed and A. Ibrahim, "Advance artificial intelligence technique for designing double T-shaped monopole antenna," *Computers, Materials & Continua*, vol. 69, no. 3, pp. 2983–2995, 2021.
[26] A. Ibrahim, S. Mirjalili, M. El-Said, S. S. M. Ghoneim, M. Al-Harthi *et al.,* "Wind speed ensemble forecasting based on deep learning using adaptive dynamic optimization algorithm," *IEEE Access*, vol. 9, pp. 125787–125804, 2021.
[27] E. -S. M. El-kenawy, A. Ibrahim, N. Bailek, K. Bouchouicha, M. A. Hassan *et al.,* "Sunshine duration measurements and predictions in Saharan Algeria region: An improved ensemble learning approach," *Theoretical and Applied Climatology*, vol. 2021, pp. 1–17, 2021.
[28] E. -S. M. El-kenawy, A. Ibrahim, N. Bailek, K. Bouchouicha, M. A. Hassan *et al.,* "Hybrid ensemble-learning approach for renewable energy resources evaluation in Algeria," *Computers, Materials & Continua*, vol. 71, no. 3, pp. 5837–5854, 2022.
[29] E. Hassib, A. El-Desouky, L. Labib and E. S. M. El-kenawy, "WOA+ BRNN: An imbalanced big data classification framework using Whale optimization and deep neural network," *Soft Computing*, vol. 24, no. 8, pp. 5573–5592, 2019.
[30] S. Mirjalili and A. Lewis, "The whale optimization algorithm," *Advances in Engineering Software*, vol. 95, no. 12, pp. 51–67, 2016.
[31] D. S. Khafaga, A. A. Alhussan, E. M. El-kenawy, A. E. Takieldeen, T. M. Hassan *et al.,* "Meta-heuristics for feature selection and classification in diagnostic breast cancer," *Computers, Materials & Continua*, vol. 73, no. 1, pp. 749–765, 2022.
[32] V. N. Vapnik, *Statistical Learning Theory*, Newyork: Wiley-Interscience Publication John Wiley & Sons, Inc., 1998.
[33] M. M. Singh, A. Singh and J. K. Manda, "A snapshot of black-hole attack detection in MANET," *International Journal of Computer Applications*, vol. 116, no. 14, pp. 23–26, 2015.
[34] M. Singh and P. Singh, "Black-hole attack detection in MANET using mobile trust points with clustering," *Communications in Computer and Information Science*, vol. 628, pp. 565–572, 2016.
[35] H. Hassan, A. I. El-Desouky, A. Ibrahim, E. M. El-kenawy and R. Arnous, "Enhanced QoS-based model for trust assessment in cloud computing environment," *IEEE Access*, vol. 8, pp. 43752–43763, 2020.
[36] A. Abdelhamid and S. R. Alotaibi, "Robust prediction of the bandwidth of metamaterial antenna using deep learning," *Computers, Materials & Continua*, vol. 72, no. 2, pp. 2305–2321, 2022.
[37] E. Hassib, A. El-Desouky, E. -S. El-kenawy and S. Elghamrawy, "An imbalanced big data mining framework for improving optimization algorithms performance," *IEEE Access*, vol. 7, pp. 170774–170795, 2019.
[38] E. M. El-Kenawy, S. Mirjalili, F. Alassery, Y. Zhang, M. Eid *et al.,* "Novel meta-heuristic algorithm for feature selection, unconstrained functions and engineering problems," *IEEE Access*, vol. 10, pp. 40536–40555, 2022.
[39] A. Takieldeen, E. M. El-kenawy, E. Hadwan and M. Zaki, "Dipper throated optimization algorithm for unconstrained function and feature selection," *Computers, Materials & Continua*, vol. 72, no. 1, pp. 1465–1481, 2022.